

UNITED STATES PATENT APPLICATION

of

Leon Wong,

Sudhanshu Aggarwal,

Peter Beebee, and

Jesse Vincent

for

**METHODS AND SYSTEMS FOR
SELECTING METHODOLOGY FOR
AUTHENTICATING COMPUTER SYSTEMS
ON A PER COMPUTER SYSTEM OR PER USER BASIS**

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

BACKGROUND OF THE INVENTION

1. Cross-Reference to Related Applications

The present application claims the benefit of United States provisional application serial number 60/186,255, filed 29 February 2000, which provisional application is incorporated herein by reference.

2. The Field of the Invention

The present invention relates to the field of electronic communication. In particular, the present invention relates to methods and systems for selecting methodology for authenticating computer systems on a per computer system or per user basis.

3. The Prior State of the Art

"Authentication" is a process often used in computer networks whereby an item is determined to be what it is purported to be. Computer networks often use authentication when computer systems communicate with each other. Typically, a first computer system will use a request/response protocol to communicate with a second computer system. To accomplish this communication, the requesting computer system establishes a connection with the responding computer system. Next, the requesting computer system transmits certain requests to the responding computer system. The responding computer system will typically respond to these requests. Often, the response to the request will depend on the identity of the requesting computer system. Thus, the responding computer system often authenticates the identity of the requesting computer system in order to determine the appropriate response. In so doing, the requesting computer system may need to provide information to the responding computer system such as a password.

1 There are a variety of methodologies for authenticating a computer system. One
2 method is to simply believe the requesting computer system is what it purports to be. This
3 method will be referred to in this description and in the claims as the "assertion" method.

4 In another method often termed the "basic HTTP" authentication method, the
5 requesting computer system sends a password over the computer network to the
6 responding computer system. The responding computer system assumes that only the
7 requesting computer system is aware of the correct password. Therefore, the responding
8 computer system concludes that the request indeed came from the requesting computer
9 system if the password is correct.

10 In a more recent HTTP authentication method termed the "MD5 Message Digest
11 Authentication" method (hereinafter, "the digest" method), the password is not passed over
12 the computer network at all. Instead, a series of numbers is generated based on a candidate
13 password and other information about the request. These numbers are then hashed using
14 the well-known MD5 hashing algorithm to form a "digest". The requesting computer
15 system then sends the digest over the computer network to the responding computer
16 system. The responding computer system takes the password that it knows to be correct,
17 and forms its own digest by performing the same method on the correct password as the
18 requesting computer system performed on the candidate password. The digest generated
19 by the requesting computer system is then compared with the digest generated by the
20 responding computer system. If the digests match, the responding computer system
21 determines that the alleged requesting computer system also generated the digest based on
22 the correct password and thus is indeed the authentic requesting computer system.

23 One authentication method that is native to WINDOWS NT ® is termed the
24 WINDOWS NT ® LAN Manager or "NTLM" authentication method. In this method, the

1 requesting computer system sends "credentials" including a user name and an encrypted
2 password to the responding computer system.

3 The abilities of the requesting computer system (and the responding computer
4 system) to handle certain authentication methods will differ from requesting computer
5 system to requesting computer system and user to user.

6 For example, some requesting computer systems and users may have permissions
7 to perform sensitive operations. It would seem inappropriate, even dangerous, to allow
8 such requesting computer systems to authenticate using the untrustworthy assertion
9 method. However, the assertion method may be entirely appropriate for requesting
10 computer systems that only have permission to perform harmless operations.

11 Some authentication methods require common knowledge of passwords between
12 the requesting computer system and the responding computer system. However,
13 oftentimes the responding computer system will have no idea of the correct password for
14 certain computer systems such as those residing outside of the responding computer
15 system's corporate network. Thus, authentication methods that require common password
16 knowledge may inappropriately deny service in some instances to requesting computer
17 systems that lie outside of the corporate network. Therefore, what are desired are methods
18 and systems for reducing denials of service to requesting computer systems that should
19 have access to the service.

20 Even if the requesting client computer system can authenticate using one of the
21 authentication methodologies accepted by the responding computer system, the requesting
22 client computer system may try several unacceptable authentication methods first before
23 finally trying one that is acceptable. Therefore, what are also desired are methods and
24 systems for improving authentication efficiency.

SUMMARY OF THE INVENTION

The present invention relates to methods and systems for selecting authentication methodology to be used on a per computer system or on a per user basis. When a client computer system makes a request for service to a server computer system, the server often needs to authenticate the client before determining whether or not service should be granted. Sometimes, the client is not capable of authenticating using the authentication method or methods accepted by the server even if the client is what it claims to be. This will often result in a denial of service even though the client may have been entitled to the service if only it could authenticate.

By allowing the authentication methodology to be selected on a per computer system or on a per user basis, acceptable authentication methodologies may be more closely tailored to match the rights given to any given requesting computer system or user. For example, requesting computer systems that only have rights to perform harmless operations may be allowed to authenticate using an untrustworthy authentication method, while requesting computer systems that have rights to perform highly sensitive operations may be required to authenticate using more trustworthy authentication methods.

In addition, the principles of the present invention enable the acceptable authentication methodologies to more closely match the ability of the particular requesting computer system or user to authenticate and the ability of the responding computer system to authenticate the particular requesting computer system. For example, the responding computer system may have no knowledge of the correct password of requesting computer systems that reside outside of its immediate network. Thus, the responding computer system will be unable to authenticate any external requesting computer systems using authentication methodologies that require common password knowledge. According, if

1 appropriate, the acceptable authentication methodologies for these computer systems may
2 be selected to include authentication methodologies that do not require common password
3 knowledge. Since the authentication methodologies can be selected on a per computer
4 system and on a per user basis, the authentication methodologies may be selected to more
5 closely match the rights and abilities of the requesting computer system and user. Thus,
6 denials of service can potentially be reduced if authentication methods are so chosen.
7 Also, authentication efficiency may be improved since the authentication ability of the
8 requesting computer system may be considered when tailoring authentication methods.
9 Thus, requesting computer system may be less likely to try numerous unsuccessful
10 authentication methods before finally authenticating with an acceptable authentication
11 method.

12 In accordance with the principles of the present invention, a computer system
13 generates a request that includes an instruction identifying the authentication method or
14 methods to be used when authenticating a subset of the client computer systems or users
15 network connected to the server computer system. The subset of client computer systems
16 may include as little as a single solitary computer system or user. The request is then
17 transmitted to the server computer system. When receiving subsequent requests for service
18 from any of the subset of client computer systems or users, the server computer system
19 will refer to the information in the instruction to determine which authentication methods
20 are acceptable in authenticating the client computer system. Thus, the present invention
21 enables fine grain control over the authentication methods used for individual computer
22 systems and users.

23 Additional features and advantages of the invention will be set forth in the
24 description which follows, and in part will be obvious from the description, or may be

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

1 learned by the practice of the invention. The features and advantages of the invention may
2 be realized and obtained by means of the instruments and combinations particularly
3 pointed out in the appended claims. These and other features of the present invention will
4 become more fully apparent from the following description and appended claims, or may
5 be learned by the practice of the invention as set forth hereinafter.

BRIEF DESCRIPTION OF THE DRAWINGS

In order that the manner in which the above-recited and other advantages and features of the invention are obtained, a more particular description of the invention briefly described above will be rendered by reference to specific embodiments thereof which are illustrated in the appended drawings. Understanding that these drawings depict only typical embodiments of the invention and are not therefore to be considered to be limiting of its scope, the invention will be described and explained with additional specificity and detail through the use of the accompanying drawings in which:

Figure 1 illustrates an exemplary system that provides a suitable operating environment for the present invention;

Figure 2 is illustrates in more detail a client/server computer network that may be used in the operating environment of Figure 1;

Figure 3 illustrates a data structure that stores and tracks the authentication methods that may be used to track each of the client computer systems of Figure 2;

Figure 4 illustrates a flowchart of a method of selecting authentication methods on a per computer system basis; and

Figure 5 illustrates in detail the data structure of a request used to make the selection of authentication methods.

DETAILED DESCRIPTION OF THE INVENTION

The present invention extends to both methods and systems for selecting methodology for authenticating on a per computer system or on a per user basis. The embodiments of the present invention may comprise a special purpose or general purpose computer including various computer hardware, as discussed in greater detail below.

Embodiments within the scope of the present invention also include computer-readable media for carrying or having computer-executable instructions or data structures stored thereon. Such computer-readable media can be any available media which can be accessed by a general purpose or special purpose computer. By way of example, and not limitation, such computer-readable media can comprise physical storage mediums such as RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to carry or store desired program code means in the form of computer-executable instructions or data structures and which can be accessed by a general purpose or special purpose computer. When information is transferred or provided over a network or another communications connection (either hardwired, wireless, or a combination of hardwired or wireless) to a computer, the computer properly views the connection as a computer-readable medium. Thus, any such a connection is properly termed a computer-readable medium. Combinations of the above should also be included within the scope of computer-readable media. Computer-executable instructions comprise, for example, instructions and data which cause a general purpose computer, special purpose computer, or special purpose processing device to perform a certain function or group of functions.

Figure 1 and the following discussion are intended to provide a brief, general description of a suitable computing environment in which the invention may be

1 implemented. Although not required, the invention will be described in the general context
2 of computer-executable instructions, such as program modules, being executed by
3 computers in network environments. Generally, program modules include routines,
4 programs, objects, components, data structures, etc. that perform particular tasks or
5 implement particular abstract data types. Computer-executable instructions, associated
6 data structures, and program modules represent examples of the program code means for
7 executing steps of the methods disclosed herein. The particular sequence of such
8 executable instructions or associated data structures represent examples of corresponding
9 acts for implementing the functions described in such steps.

10 Those skilled in the art will appreciate that the invention may be practiced in
11 network computing environments with many types of computer system configurations,
12 including personal computers, hand-held devices, multi-processor systems,
13 microprocessor-based or programmable consumer electronics, network PCs,
14 minicomputers, mainframe computers, and the like. The invention may also be practiced
15 in distributed computing environments where tasks are performed by local and remote
16 processing devices that are linked (either by hardwired links, wireless links, or by a
17 combination of hardwired or wireless links) through a communications network. In a
18 distributed computing environment, program modules may be located in both local and
19 remote memory storage devices.

20 With reference to Figure 1, an exemplary system for implementing the invention
21 includes a general purpose computing device in the form of a conventional computer 120,
22 including a processing unit 121, a system memory 122, and a system bus 123 that couples
23 various system components including the system memory 122 to the processing unit 121.
24 The system bus 123 may be any of several types of bus structures including a memory bus

1 or memory controller, a peripheral bus, and a local bus using any of a variety of bus
2 architectures. The system memory includes read only memory (ROM) 124 and random
3 access memory (RAM) 125. A basic input/output system (BIOS) 126, containing the basic
4 routines that help transfer information between elements within the computer 120, such as
5 during start-up, may be stored in ROM 124.

6 The computer 120 may also include a magnetic hard disk drive 127 for reading
7 from and writing to a magnetic hard disk 139, a magnetic disk drive 128 for reading from
8 or writing to a removable magnetic disk 129, and an optical disk drive 130 for reading
9 from or writing to removable optical disk 131 such as a CD-ROM or other optical media.
10 The magnetic hard disk drive 127, magnetic disk drive 128, and optical disk drive 130 are
11 connected to the system bus 123 by a hard disk drive interface 132, a magnetic disk drive-
12 interface 133, and an optical drive interface 134, respectively. The drives and their
13 associated computer-readable media provide nonvolatile storage of computer-executable
14 instructions, data structures, program modules and other data for the computer 120.
15 Although the exemplary environment described herein employs a magnetic hard disk 139,
16 a removable magnetic disk 129 and a removable optical disk 131, other types of computer
17 readable media for storing data can be used, including magnetic cassettes, flash memory
18 cards, digital video disks, Bernoulli cartridges, RAMs, ROMs, and the like.

19 Program code means comprising one or more program modules may be stored on
20 the hard disk 139, magnetic disk 129, optical disk 131, ROM 124 or RAM 125, including
21 an operating system 135, one or more application programs 136, other program modules
22 137, and program data 138. A user may enter commands and information into the
23 computer 120 through keyboard 140, pointing device 142, or other input devices (not
24 shown), such as a microphone, joy stick, game pad, satellite dish, scanner, or the like.

1 These and other input devices are often connected to the processing unit 121 through a
2 serial port interface 146 coupled to system bus 123. Alternatively, the input devices may
3 be connected by other interfaces, such as a parallel port, a game port or a universal serial
4 bus (USB). A monitor 147 or another display device is also connected to system bus 123
5 via an interface, such as video adapter 148. In addition to the monitor, personal computers
6 typically include other peripheral output devices (not shown), such as speakers and
7 printers.

8 The computer 120 may operate in a networked environment using logical
9 connections to one or more remote computers, such as remote computers 149a and 149b.
10 Remote computers 149a and 149b may each be another personal computer, a server, a
11 router, a network PC, a peer device or other common network node, and typically includes
12 many or all of the elements described above relative to the computer 120, although only
13 memory storage devices 150a and 150b and their associated application programs 136a and
14 136b have been illustrated in Figure 1. The logical connections depicted in Figure 1
15 include a local area network (LAN) 151 and a wide area network (WAN) 152 that are
16 presented here by way of example and not limitation. Such networking environments are
17 commonplace in office-wide or enterprise-wide computer networks, intranets and the
18 Internet.

19 When used in a LAN networking environment, the computer 120 is connected to
20 the local network 151 through a network interface or adapter 153. When used in a WAN
21 networking environment, the computer 120 may include a modem 154, a wireless link, or
22 other means for establishing communications over the wide area network 152, such as the
23 Internet. The modem 154, which may be internal or external, is connected to the system
24 bus 123 via the serial port interface 146. In a networked environment, program modules

1 depicted relative to the computer 120, or portions thereof, may be stored in the remote
2 memory storage device. It will be appreciated that the network connections shown are
3 exemplary and other means of establishing communications over wide area network 152
4 may be used.

5 Figure 2 illustrates a suitable network 200 in which the present invention may
6 operate and will be referred to frequently in describing embodiments of the present
7 invention. The network 200 includes a server computer system 210 that is network
8 connected to a plurality of client computer systems 220 including five client computer
9 systems 220a through 220e. Each of the server computer system 210 and the client
10 computer systems 220a through 220e may be structured as described above for the
11 computer 120 of Figure 1 and include some or all of the components described as being
12 included in the computer 120. However, many other computer devices may be used as the
13 server computer system and client computer systems so long as they are capable of
14 implementing the principles of the present invention as described herein.

15 In order to facilitate a clear understanding of the principles of the present invention,
16 certain terms are hereinafter defined which are intended to be applied throughout this
17 description and in the following claims.

18 In this description and in the claims, an "entity for authentication" is defined as a
19 client computer system or user thereof which is to be authenticated.

20 In this description and in the following claims, a "client computer system" is
21 defined as a computer or group of computers that uses the services of another computer
22 system. A "server computer system" is defined as a computer or group of computers that
23 provides services to another computer system. A "computer" is defined as any device
24

1 capable of processing data such as a personal computer, a personal digital assistant, and the
2 like.

3 Note that a computer system may use the services of another computer system and
4 yet still provide services to yet other computer systems. Thus, a client computer system in
5 one context may also be a server computer system in another context. Similarly, a server
6 computer system in one context may also be a client computer system in another context.
7 The use of the term "server computer system" for computer system 210 and "client
8 computer system" for computer systems 220a through 220e is intended in the context of
9 authentication. In other words, the computer system 210 is a server computer system
10 because it serves by authenticating. The computer systems 220a through 220e are client
11 computer systems because they are served by the server computer system 210
12 authenticating. The use of the term "server computer system" for the server computer
13 system 210 is not intended to imply that the server computer system 210 cannot also be a
14 client computer system in a different context. Similarly, the use of the term "client
15 computer system" for the client computer systems 220a through 220e is not intended to
16 imply that the client computer systems cannot also be server computer systems in a
17 different context.

18 In this description and in the following claims, "network connected" means having
19 a connection either directly or indirectly through one or more networks. The solid line
20 connecting each of client computer systems 220a through 220e to the server computer
21 system 210 represents that these client computer systems are network connected to the
22 server computer system 210.

23 As each of the client computer systems 220 make a request to the server computer
24 system 210, the server computer system 210 will perform services to authenticated client

1 computer systems 220. Such as service may include, for example, access to presence
2 information for use in instant messaging, the retrieval of a file, or the like.

3 The server computer system 210 is capable of performing authentication using any
4 one or more of authentication methods 211, 212, 213 and 214. As an example, suppose
5 that authentication method 211 is the "assertion" method, method 212 is the "basic HTTP"
6 method, method 213 is the "digest" method, and method 214 is the NTLM method.

7 Many of the client computer systems are not able to authenticate using all of these
8 authentication methods. For example, some may not be able to authenticate to the server
9 computer system 210 using certain methods since the server computer system 210 lacks
10 certain information such as passwords necessary for the server computer system to verify
11 the identity of the client computer system. Others may not be able to authenticate certain
12 methods due to technical limitations of the client computer system itself.

13 Referring to Figure 2, client computer systems 220a and 220e have the ability to
14 authenticate to the server computer system 210 using any one or more of the authentication
15 methods 211, 212, 213 and 214.

16 However, due to technical limitations within the client computer system 220b itself,
17 the client computer system 220b can only authenticate using authentication methods
18 211 and 212, but not authentication methods 213 and 214.

19 Client computer systems 220c and 220d are fairly sophisticated and generally have
20 the ability to authenticate using authentication methods 211, 212, 213 and 214. However,
21 the client computer systems 220c and 220d can only authenticate to the server computer
22 system 210 using authentication method 211. Dashed boxes are use to identify
23 authentication methods which the client computer system is generally capable of but which
24 cannot be used to authenticate to the server computer system 210. For example, suppose

1 that the server computer system 210 does not have knowledge of the correct passwords for
2 client computer systems 220c and 220d, the client computer systems 220c and 220d would
3 be unable to authenticate to the server computer system 210 using any authentication
4 which requires knowledge of passwords.

5 Suppose that, although the server computer system 210 has the potential ability to
6 authenticate using any one of authentication methods 211, 212, 213 and 214, the server
7 computer system 210 is configured to authenticate using only the "digest" method 213 and
8 "ntlm" method. In this case, client computer systems 220b, 220c and 220d would not be
9 able to authenticate to the server computer system 210. Thus, client computer systems
10 220b, 220c and 220d would be denied service even though they should have access to the
11 service if only they could authenticate themselves to the server computer system 210.

12 Now suppose that the server computer system 210 supports authentication methods
13 211, 212, 213 and 214. Suppose further that client computer systems 220c and 220d are
14 both configured to try to authenticate using method 214. If unsuccessful, the client
15 computer system would then try method 213, then method 212, and finally the assertion
16 method 211. Authentication of client computer systems 220c and 220d would each require
17 three unsuccessful authentication attempts before finally succeeding with method 211.

18 In accordance with the principles of the present invention, authentication efficiency
19 can be improved and denials of service can be reduced by selecting the authentication
20 methodologies that the server computer system 210 is to use on a per computer system
21 basis (or on a per user basis) depending on the authentication abilities of each of the client
22 computer systems and depending on the rights of the computer systems

23 Suppose that some client computer systems have rights to perform highly sensitive
24 operations using the server computer system 210. In this case, conventional wisdom

1 would require the server computer system 210 be restricted to authentication methods that
2 are reliable. The assertion method 211, for example, would be highly unreliable as that
3 would require that the server computer system 210 simply believe the client computer
4 system was what it is purported to be. If the server computer system 210 only allowed
5 authentication using reliable methods, client computer systems 220c and 220d could never
6 authenticate to the server computer system 210 even if they only had rights to perform
7 harmless operations. The present invention allows for the selection of authentication
8 methods on a per computer system basis and on a per user basis to take into consideration
9 the rights of the associated client computer system.

10 Figure 3 illustrates a data structure 300 that is accessible by the server computer
11 system 210 and which is used to allow the authentication methods to be selected on a per
12 computer system basis and/or on a per user basis. The data structure 300 includes a client
13 identifier field 310 which identifies the client computer systems 220a through 220e. The
14 client identifier field 310 could also identify users. The data structure also includes
15 authentication fields 320 which identify the acceptable authentication methods for the
16 corresponding client computer system. In Figure 3, the authentication fields 320 contain a
17 flag for each authentication method including assertion flag 321, basic HTTP flag 322,
18 digest flag 323 and NTLM flag 324. The setting of a flag is represented by a check mark
19 indicating that the corresponding authentication method is acceptable when authenticating
20 that particular client computer system or user.

21 For example, referring to the first row of the data structure 300, acceptable
22 authentication methods for client computer system 220a are the relatively reliable digest
23 and NTLM methods. Less reliable authentication methods including the assertion and
24 basic HTTP methods are not accepted as illustrated by the lack of a check mark for these

1 fields. The client computer system 220a may have rights to perform highly sensitive
2 operations using the server computer system 210. Therefore, it was appropriate that only
3 reliable authentication methods be used to authenticate the client computer system 210.

4 Upon authentication, the server computer system 210 may communicate to the
5 client computer system 220a the acceptable authentication methods. This allows the client
6 computer system 220a to authenticate using acceptable authentication methods without
7 going through the inefficiencies of first trying unacceptable authentication methods such as
8 methods 211 and 212.

9 Referring to the second row of the data structure, acceptable authentication
10 methods for the client computer system 220b also include only the reliable authentication
11 methods 213 and 214 since the client computer system 220b has rights to perform sensitive
12 operations using the server computer system 210. However, note that the client computer
13 system 220b is not capable of authenticating using any of methods 213 and 214 to the
14 server computer system 210. Accordingly, client computer system 220b will ultimately be
15 denied service since acceptable authentication is not possible. However, the server
16 computer system 210 would communicate the acceptable authentication methods to the
17 client computer system 220b. The client computer system 220b could then infer the
18 futility of trying to authenticate using methods 211 and 212 thereby efficiently concluding
19 that authentication is denied without even having tried methods 211 or 212. If desired, the
20 methods described herein may be used to alter the data structure so as to allow the client
21 computer system 220b to use methods 211 and 212 to authenticate to the server computer
22 system 210.

23 Proceeding down the data structure, acceptable authentication methods for client
24 computer systems 220c and 220d include only the least reliable authentication method,

1 assertion method 211. Client computer systems 220c and 220d may only have rights to
2 perform harmless operations using the server computer system 210. Accordingly, it is
3 appropriate that the client computer systems 220c and 220d be allowed to authenticate
4 using any method they so choose. However, the server computer system 210 may lack
5 information such as passwords necessary to authenticate client computer systems 220c and
6 220d using methods 212, 213 and 214. Accordingly, these methods 212, 213 and 214 are
7 not designated as acceptable methods. During authentication, the server computer system
8 210 may communicate that the assertion method 211 is the only acceptable authentication
9 method for the respective client computer systems 220c and 220d. In this case, the client
10 computer systems 220c and 220d may forego attempts to try to authenticate using methods
11 212, 213 and 214. Instead, the client computer system 220c and 220d may immediately
12 authenticate using the accepted assertion method 211 thereby foregoing the inefficiencies
13 of having to first try unacceptable authentication methods.

14 In addition to the efficiency advantages, refraining from attempting unacceptable
15 authentication methods has certain security advantages as well. For example, some
16 methods of authentication including basic authentication reveal the user's password to the
17 network. Thus, attempting basic authentication if basic authentication is not going to work
18 would result in unnecessarily risking the revealing of the password.

19 Proceeding to the last row of the data structure 300, acceptable authentication
20 methods for the client computer system 220e include all authentication methods 211, 212,
21 213 and 214. Accordingly, the client computer system 220e could authenticate using any
22 of these authentication methods.

23 The structure of Figures 1, 2 and 3 represents a system in which and with which the
24 present invention may operate. Although the server computer system 210 is network

1 connected to five client computer systems in Figure 2, the server computer system 210
2 may be network connectable to more or less than five client computer systems.
3 Furthermore, the server computer system 210 may be connected to other server computer
4 systems. In one example operating environment, the server computer system 210 is part of
5 the constellation of computer systems that form the Internet.

6 Figure 4 illustrates a method 400 for selecting authentication methods to be used by
7 the server computer system 210 on a per computer system basis. In other words, the
8 claimed identity of the computer system will determine which authentication methods may
9 be used to authenticate that computer system. In the following example, the client
10 computer system 220e of Figure 2 controls which authentication methods will be
11 acceptable for each client computer system 220a through 220e. However, the control of
12 the authentication methods may come from other computer systems as well.

13 In the method of Figure 4, acts performed exclusively by the client computer
14 system that controls which authentication methods are used (hereinafter, the "controlling
15 client computer system) such as the client computer system 220e are listed directly below
16 the heading "CLIENT" on the left-hand side of Figure 4. Acts performed exclusively by
17 the server computer system 210 are listed directly below the heading "SERVER" on the
18 right-hand side of Figure 4.

19 Referring to Figure 4, the controlling client computer system creates a request that
20 includes a selection of acceptable authentication methods (act 410) to be used against at
21 least a subset of the plurality of client computer systems 220 when those client computer
22 system request a service.

23 Figure 5 illustrates a data structure 500 of a request to select authentication
24 methods. The data structure includes one or more access control element fields 510a

1 through 510n. Each access control element field includes a client identifier field 512 that
2 identifies the subset of client computer systems or users to which the authentication
3 methods are to be applied. The subset of client computer systems may include as few as a
4 single client computer system. In addition, each access control element field includes an
5 authentication field 514 that identifies the authentication types used to authenticate the
6 identified subset. Although these fields 512 and 514 are only shown for the first access
7 control element field 510a, the other access control elements fields may each include
8 similar fields for additional client computer systems and/or users.

9 The data structure 500 of the request may include an eXtensible Markup Language
10 (XML) element or any other data structure that identifies the authentication methods and
11 the computer systems and/or users to which those authentication methods will be applied.
12 Take the following XML element as an example.

```
13  
14 <?xml version="1.0"?>  
15 <a:rvpacl xmlns:a="http://schemas.microsoft.com/rvp/acl">  
16     <a:acl>  
17         <a:inheritance>none</a:inheritance>  
18         <a:ace>  
19             <a:principal>  
20                 <a:rvp-principal>  
21                     http://im.example.com/instmsg/aliases/220b/  
22                 </a:rvp-principal>  
23                 <a:credentials>  
24                 <a:digest>
```

1 <a:ntlm/>
 2 </a:credentials>
 3 </a:principal>
 4 </a:ace>
 5 </a:acl>
 6 </a:rvpac1>
 7

8 In this XML element, the portion between <a:ace> and </a:ace> defines an Access
 9 Control Element (ACE) that defines access permissions. This portion would correspond to
 10 the access control element field 510a shown in Figure 5. The portion of the access control
 11 element that occurs between <a:rvp-principal> and </a:rvp-principal> defines the entity to
 12 whom the access permission is to apply (corresponds to the client identifier field 512 of
 13 Figure 5). In the above example request, the Uniform Resource Locator (URL)
 14 corresponding to the entity is "http://im.example.com/instmsg/aliases/220b/" which
 15 represents client computer system 220b. The portion of the access control element that
 16 occurs between <a:credentials> and </a:credentials> describes authentication mechanisms
 17 that may be used to authenticate the client computer system 220b when requesting access
 18 to services (corresponds to the authentication field 514 of Figure 5). This portion describes
 19 the two authentication methods that may be used when authenticating the client computer
 20 system 220b. Specifically, "<a:digest/>" means that the "digest" authentication method is
 21 acceptable while "<a:ntlm/>" means that the "ntlm" method is also acceptable.

22 Once the controller client computer system generates the request to select
 23 authentication methods (act 410), the controller client computer system then transmits the
 24 request to the server computer system (act 420). For example, the controller client

1 computer system 220e may transmit to the server computer system 210 the request to
2 allow the "digest" and "ntlm" authentication methods for authenticating client computer
3 system 220b.

4 Once the request is received at the server computer system (act 430), subsequent
5 requests for a service will result in the server computer system authenticating the client
6 computer system using the authentication methods identified in the authentication selection
7 request previously received from the controlling client computer system. Accordingly,
8 embodiments within the scope of the present invention include a means or step for the
9 server computer system authenticating the subset of the client computer systems using at
10 least the authentication methodology identified in the instruction.

11 In one embodiment, the server computer system sets the appropriate authentication
12 flags for the corresponding client computer system within the data structure 500 to
13 represent the new authentication methods (act 440). Then, upon receiving subsequent
14 requests for services, the server computer system determines how to authenticate based on
15 the authentication flags within the data structure 500 (act 450). Although a specific
16 example of a data structure that stores the authentication methods that are to be used for
17 each client computer system, any data structure that can be referred to in determining the
18 appropriate authentication methods will suffice.

19 The above describes methods and systems for selecting authentication methods on
20 a per computer system basis and on a per user basis. Since the authentication methods may
21 be tailored to each computer system, there may be fewer service denials due to
22 authentication failure, and more efficient authentication.

23 The present invention may be embodied in other specific forms without departing
24 from its spirit or essential characteristics. The described embodiments are to be considered

1 in all respects only as illustrative and not restrictive. The scope of the invention is,
2 therefore, indicated by the appended claims rather than by the foregoing description. All
3 changes which come within the meaning and range of equivalency of the claims are to be
4 embraced within their scope.

5 What is claimed and desired to be secured by United States Letters Patent is:
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24